

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-124941

(43)Date of publication of application : 26.04.2002

(51)Int.Cl.

H04L 9/08

H04L 12/28

(21)Application number : 2000-317630

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 18.10.2000

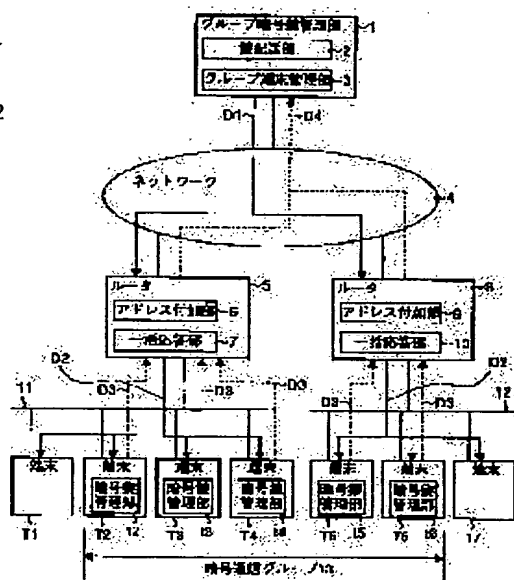
(72)Inventor : TOKIWA YASUHIRO  
ATOZAWA SHINOBU

## (54) ENCRYPTION COMMUNICATION SYSTEM AND METHOD FOR DELIVERING ENCODING KEY

(57)Abstract:

PROBLEM TO BE SOLVED: To alleviate a load on a network at delivery responding of an encoding key used for an encryption communication group.

SOLUTION: A group encryption key managing unit 1 generates a group key, and transmits the key to terminal units T2 to T6 belonging to a communication group 13 via a router 5 and a router 8. The terminal units T2 to T6 transmit delivery response data D3 for transmitting reception of the group key to the router 5. The router 5 transmits the data as a simultaneous response data D4 to the unit 1 based on the data D3. The units T5 and T6 transmit the data D3 for transmitting the reception of the key to the router 8. The router 8 transmits the data D3 to the unit 1 as the data D4 based on the data D3.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C): 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-124941  
(P2002-124941A)

(43) 公開日 平成14年4月26日 (2002.4.26)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B 5 J 1 0 4
12/28		11/00	3 1 0 Z 5 K 0 3 3

審査請求 未請求 請求項の数12 O L (全 22 頁)

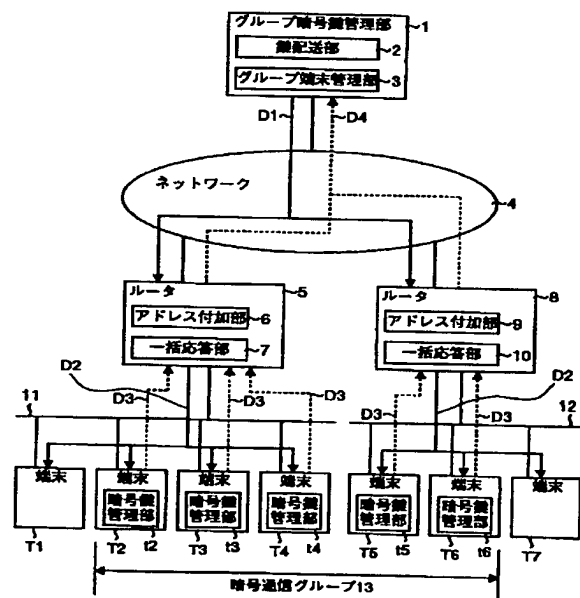
(21) 出願番号	特願2000-317630 (P2000-317630)	(71) 出願人	000006013 三菱電機株式会社 東京都千代田区丸の内二丁目2番3号
(22) 出願日	平成12年10月18日 (2000. 10. 18)	(72) 発明者	時庭 康久 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
		(72) 発明者	後沢 忍 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
		(74) 代理人	100089118 弁理士 酒井 宏明
		Fターム (参考)	5J104 AA16 BA02 EA01 EA04 EA18 MA06 NA02 PA07 5K033 AA03 AA08 BA13 CB01 DA03

(54) 【発明の名称】 暗号通信システムおよび暗号鍵配送方法

## (57) 【要約】

【課題】 暗号通信グループが用いる暗号鍵の配送応答時におけるネットワークの負担を軽減すること。

【解決手段】 グループ暗号鍵管理部1がグループ暗号鍵を生成し、ルータ5およびルータ8を介して暗号通信グループ13に属する端末T2～T6に送信する。端末T2～T4は、グループ暗号鍵を受信したことを伝える配送応答データD3をルータ5に送信し、ルータ5は、配送応答データD3をもとに、一括応答データD4としてグループ暗号鍵管理部1に送信する。端末T5、T6は、グループ暗号鍵を受信したことを伝える配送応答データD3をルータ8に送信し、ルータ8は、配送応答データD3をもとに、一括応答データD4としてグループ暗号鍵管理部1に送信する。



## 【特許請求の範囲】

【請求項1】 グループ暗号鍵を用いた暗号通信が行われる暗号通信グループを形成する複数の端末が中継手段を介してネットワークに接続され、該ネットワークに接続されたグループ暗号鍵管理手段が前記グループ暗号鍵を生成し、前記中継手段を介して各端末に配送する暗号通信システムにおいて、

前記グループ暗号鍵管理手段は、

前記生成したグループ暗号鍵を含む鍵配送データを前記各端末に一斉に送信する鍵配送手段と、

前記中継手段から受信した一括応答データをもとに、前記暗号通信グループを形成する前記各端末が前記グループ暗号鍵を受信したか否かを管理するグループ端末管理手段とを備え、

前記中継手段は、

前記鍵配送データに代理応答アドレスとして自中継手段のアドレスを付加し、鍵配送終端データとして自中継手段が中継する前記端末に送信するアドレス付加手段と、前記端末から受信した配送応答データをもとに、前記グループ暗号鍵を受信した端末の情報を含む前記一括応答データを前記グループ暗号鍵管理手段に送信する一括応答手段とを備え、

前記端末は、

前記鍵配送終端データを受信して前記グループ暗号鍵を受信し、自端末の情報を含む前記配送応答データを前記中継手段に送信する暗号鍵管理手段を備えることを特徴とする暗号通信システム。

【請求項2】 前記一括応答手段は、前記一括応答データに含まれる端末の情報を暗号化する第1の暗号化手段をさらに備え、

前記グループ端末管理手段は、前記一括応答データに含まれる暗号化された端末の情報を復号する第1の復号手段をさらに備えることを特徴とする請求項1に記載の暗号通信システム。

【請求項3】 前記暗号鍵管理手段は、前記配送応答データに含まれる自端末の情報を暗号化する第2の暗号化手段をさらに備え、

前記一括応答手段は、前記配送応答データに含まれる暗号化された情報を復号する第2の復号手段をさらに備えることを特徴とする請求項1または2に記載の暗号通信システム。

【請求項4】 前記第1の暗号化手段、前記第2の暗号化手段、前記第1の復号手段、および前記第2の復号手段は、秘密鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする請求項2または3に記載の暗号通信システム。

【請求項5】 前記第1の暗号化手段、前記第2の暗号化手段、前記第1の復号手段、および前記第2の復号手段は、公開鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする請求項2または3に記載の暗

号通信システム。

【請求項6】 前記第1の暗号化手段、前記第2の暗号化手段、前記第1の復号手段、および前記第2の復号手段は、既に配送されたグループ暗号鍵を少なくとも保持し、この保持されたグループ暗号鍵のうちの所定のグループ暗号鍵を用いて暗号化または復号を行うことを特徴とする請求項2～4のいずれか一つに記載の暗号通信システム。

【請求項7】 グループ暗号鍵を用いた暗号通信が行われる暗号通信グループを形成する複数の端末が中継手段を介してネットワークに接続され、該ネットワークに接続されたグループ暗号鍵管理手段が前記グループ暗号鍵を生成し、前記中継手段を介して各端末に配送する暗号鍵配送方法において、

前記グループ暗号鍵管理手段が、前記グループ暗号鍵を含む鍵配送データを前記端末に一斉に送信する鍵配送データ送信工程と、

前記中継手段が、前記鍵配送データに代理応答アドレスとして自中継手段のアドレスを付加し、該アドレスが付加された鍵配送データを鍵配送終端データとして前記端末に送信する鍵配送終端データ送信工程と、

前記端末が、前記鍵配送終端データを受信して前記グループ暗号鍵を受信し、自端末の情報を含む配送応答データを前記中継手段に送信する配送応答データ送信工程と、

前記中継手段が、前記端末から受信した配送応答データをもとに、前記グループ暗号鍵を受信した端末の情報を含む一括応答データを前記グループ暗号鍵管理手段に送信する一括応答データ送信工程と、

前記グループ暗号鍵管理手段が、前記一括応答データをもとに、前記各端末が前記グループ暗号鍵を受信したか否かを確認する配送結果確認工程と、を含むことを特徴とする暗号鍵配送方法。

【請求項8】 前記一括応答データ送信工程は、前記一括応答データに含まれる端末の情報を暗号化する第1の暗号化工程をさらに含み、

前記配送結果確認工程は、前記一括応答データに含まれる暗号化された端末の情報を復号する第1の復号工程をさらに含むことを特徴とする請求項7に記載の暗号鍵配送方法。

【請求項9】 前記配送応答データ送信工程は、前記配送応答データに含まれる自端末の情報を暗号化する第2の暗号化工程をさらに含み、

前記一括応答データ送信工程は、前記配送応答データに含まれる暗号化された情報を復号する第2の復号工程をさらに含むことを特徴とする請求項7または8に記載の暗号鍵配送方法。

【請求項10】 前記第1の暗号化工程、前記第2の暗号化工程、前記第1の復号工程、および前記第2の復号工程は、秘密鍵暗号方式によってそれぞれ暗号化または

復号を行うことを特徴とする請求項8または9に記載の暗号鍵配送方法。

【請求項11】 前記第1の暗号化工程、前記第2の暗号化工程、前記第1の復号工程、および前記第2の復号工程は、公開鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする請求項8または9に記載の暗号鍵配送方法。

【請求項12】 前記第1の暗号化工程、前記第2の暗号化工程、前記第1の復号工程、および前記第2の復号工程は、既に配送されたグループ暗号鍵を少なくとも保持し、この保持されたグループ暗号鍵のうちの所定のグループ暗号鍵を用いて暗号化または復号を行うことを特徴とする請求項8または9に記載の暗号鍵配送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、グループ暗号鍵を用いた暗号通信が行われる暗号通信グループを形成する複数の端末が中継手段を介してネットワークに接続され、該ネットワークに接続されたグループ暗号鍵管理手段が前記グループ暗号鍵を生成し、前記中継手段を介して各端末に配送する暗号通信システムおよび暗号鍵配送方法に関し、特に、ネットワークの負担を軽減することができる暗号通信システムおよび暗号鍵配送方法に関するものである。

【0002】

【従来の技術】従来から、ネットワークに接続された端末間の通信における安全性を確保するために、端末をグループ分けし、同一のグループ内の通信を共通の暗号鍵を用いて行う暗号通信システムがある。この共通の暗号鍵は、安全性を高めるためにしばしば更新されるが、新しい暗号鍵自体も安全に各端末に配送しなければならない。

【0003】図8は、従来の暗号通信システムの構成を示す図である。この従来の暗号通信システムは、グループ暗号鍵管理部801と複数の端末810、820、830を有し、グループ暗号鍵管理部801が各端末810、820、830にグループ暗号鍵802を配送する。ここでは、端末810、820、830が、1つの暗号通信グループを形成しているものとする。グループ暗号鍵802の配送は、暗号化されて行われる。このため、グループ暗号鍵管理部801および各端末810、820、830は、配送用暗号鍵を、たとえば物理的に安全な方法で配布するなど、なんらかの手段で予め秘密に共有していなければならない。暗号通信グループに対してグループ暗号鍵を配送する場合、グループ暗号鍵を配送するグループ暗号鍵管理部801と各端末810、820、830とは、配送用暗号鍵を、それぞれ配送用暗号鍵保持部805、813に保持していなければならない。

【0004】暗号化部803および復号部814は、配

送用暗号鍵保持部805、813から入力された配送用暗号鍵を用いてグループ暗号鍵802をそれぞれ暗号化し、復号する。暗号方式としては、暗号化と復号とで同じ暗号鍵を用いる秘密鍵暗号方式を採用する。この秘密鍵暗号方式には、たとえば米国の標準暗号方式であるDES (Data Encryption Standard) などがあるが、暗号鍵を知らない者が暗号文から平文を推定できない方式であればよい。なお、ENC (M, K) およびDEC (M, K) は、鍵Kを用いて情報Mをそれぞれ暗号化し、復号する関数を表す。また、同報送信部806は、各端末810、820、830に同報送信する。また、同報受信部811は、同報送信部806から送られた同報情報を受信する。

【0005】つぎに、図9に示すフローチャートを用いてグループ暗号鍵配送時のグループ暗号鍵管理部801の動作を説明する。ある暗号通信グループにおける暗号通信の開始時に(ステップS101)、グループ暗号鍵管理部801は、まずグループ暗号鍵を生成する(ステップS102)。つぎに暗号通信グループ内の各端末それぞれについて(ステップS103)、該端末との配送用暗号鍵を配送用暗号鍵保持部805から順次取出し(ステップS104)、それぞれの配送用暗号鍵を鍵として暗号化部803でグループ暗号鍵を順次暗号化して暗号化グループ暗号鍵を計算し(ステップS105)、それらをグループ暗号鍵リスト804にまとめて(ステップS106)、同報送信部806が該リストをマルチキャスト送信する(ステップS107)。該リストは、全端末に受信される。マルチキャスト送信には、IGMP (Internet Group Management Protocol) などの標準的な通信規約を用いることができる。

【0006】つぎに、図10を用いてグループ暗号鍵配送時の端末の動作を説明する。端末810が同報受信部811によりグループ暗号鍵リスト804を受信した場合(ステップS201)、グループ暗号鍵リスト804に自端末に対応する暗号化グループ暗号鍵があれば(ステップS202, Yes)、グループ暗号鍵リスト804から暗号化グループ暗号鍵を取り出し(ステップS203)、配送用暗号鍵保持部813に保持されたグループ暗号鍵管理部801との配送用暗号鍵を取り出し(ステップS204)、配送用暗号鍵を用いて復号部814で暗号化グループ暗号鍵を復号し、グループ暗号鍵802を得る(ステップS205)。一方、受信したグループ暗号鍵リスト804の中に自端末に対応する暗号化グループ暗号鍵がない場合には(ステップS202, No)、グループ暗号鍵リスト804を無視する(ステップS206)。

【0007】つぎに、図11を用いてグループ暗号鍵リストについて具体的に説明する。グループ暗号鍵管理部801と端末810、820、830とはそれぞれ配送用暗号鍵K810、K820、K830を保持してい

る。グループ暗号鍵管理部801はグループ暗号鍵Xを生成し、各端末810、820、830との配送用暗号鍵K810、K820、K830をそれぞれ鍵として、グループ暗号鍵Xを暗号化し、暗号化されたグループ暗号鍵Y810、Y820、Y830を作成する。

【0008】すなわちグループ暗号鍵管理部801は  
Y810=ENC(X, K810)  
Y820=ENC(X, K820)  
Y830=ENC(X, K830)

を生成する。その後、グループ暗号鍵管理部801はグループ暗号鍵Y810、Y820、Y830をグループ暗号鍵リスト901(図11参照)として全端末810、820、830にマルチキャスト送信する。グループ暗号鍵リスト804は暗号通信グループに属さない端末や第三者に受信されても、その端末に対応する配送用暗号鍵がないのでグループ暗号鍵Xを推察されることはない。

【0009】一方、グループ暗号鍵管理部801からグループ暗号鍵リスト804に対応するグループ暗号鍵リスト901を受け取った端末810は、グループ暗号鍵リスト901から自端末に対応する暗号化グループ暗号鍵Y810を取り出し、グループ暗号鍵管理部801との配送用暗号鍵K810を鍵として用いて復号を行い、グループ暗号鍵Xを得る。

【0010】端末820、端末830についても同様な復号処理を行い各端末810、820、830では次のよう復号結果を得る。

端末810: X=DEC(Y810, K810)

端末820: X=DEC(Y820, K820)

端末830: X=DEC(Y830, K830)

これによって、端末810、820、830のみがグループ暗号鍵Xを受信し、グループ通信用の暗号鍵として保持し、使用する。グループ暗号鍵Xの受信後、端末810、820、830は、配送結果を一斉にグループ暗号鍵管理部801に応答する。グループ暗号鍵管理部801は、暗号通信グループに属する端末810、820、830からの配送応答によって、どの端末が正常にグループ暗号鍵Xを受信したかを知る。これによって、暗号通信グループに属するグループ暗号鍵管理部801、端末810、820、830は、グループ暗号鍵Xを共有することができる。

【0011】

【発明が解決しようとする課題】しかしながら、上述した暗号通信システムは、グループ暗号鍵を受信した端末が、グループ暗号鍵管理部への配送応答を一斉に行うので、暗号通信グループの規模が大きくなり、端末数が増えたと、グループ暗号鍵管理部での負荷が増大し、通信ネットワーク上の通信量が大きくなるという問題点があった。また、グループ暗号鍵の配送応答のセキュリティ強度を高めて暗号通信システムの安全性を高める必要が

あった。

【0012】この発明は上記に鑑みてなされたものであって、暗号通信グループがグループ暗号鍵の共有を容易に行い、かつ、ネットワークの負担を軽減し、さらにセキュリティを強化した暗号通信システムおよび暗号鍵配送方法を得ることを目的とする。

【0013】

【課題を解決するための手段】上記目的を達成するため、この発明にかかる暗号通信システムは、グループ暗号鍵を用いた暗号通信が行われる暗号通信グループを形成する複数の端末が中継手段を介してネットワークに接続され、該ネットワークに接続されたグループ暗号鍵管理手段が前記グループ暗号鍵を生成し、前記中継手段を介して各端末に配送する暗号通信システムにおいて、前記グループ暗号鍵管理手段は、前記生成したグループ暗号鍵を含む鍵配送データを前記各端末に一斉に送信する鍵配送手段と、前記中継手段から受信した一括応答データをもとに、前記暗号通信グループを形成する前記各端末が前記グループ暗号鍵を受信したか否かを管理するグループ端末管理手段とを備え、前記中継手段は、前記鍵配送データに代理応答アドレスとして自中継手段のアドレスを付加し、鍵配送終端データとして自中継手段が中継する前記端末に送信するアドレス付加手段と、前記端末から受信した配送応答データをもとに、前記グループ暗号鍵を受信した端末の情報を含む前記一括応答データを前記グループ暗号鍵管理手段に送信する一括応答手段とを備え、前記端末は、前記鍵配送終端データを受信して前記グループ暗号鍵を受信し、自端末の情報を含む前記配送応答データを前記中継手段に送信する暗号鍵管理手段を備えることを特徴とする。

【0014】この発明によれば、中継手段は、グループ暗号鍵管理手段が送信した鍵配送データに、自中継手段のアドレスを付加して各端末に配送し、各端末は、受信したデータに付加されたアドレスをもとに、自端末の情報を含む配送応答データを中継手段に送信し、中継手段は、端末から受信した配送応答データをもとに、グループ暗号鍵を受信した端末の情報をまとめ、一括応答データとしてグループ暗号鍵管理手段に送信する。

【0015】つぎの発明にかかる暗号通信システムは、上記の発明において、前記一括応答手段は、前記一括応答データに含まれる端末の情報を暗号化する第1の暗号化手段をさらに備え、前記グループ端末管理手段は、前記一括応答データに含まれる暗号化された端末の情報を復号する第1の復号手段をさらに備えることを特徴とする。

【0016】この発明によれば、中継手段はグループ暗号鍵を受信した端末の情報を暗号化してグループ暗号鍵管理手段に送信し、グループ暗号鍵管理手段は、中継手段からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができる。

【0017】つぎの発明にかかる暗号通信システムは、上記の発明において、前記暗号鍵管理手段は、前記配送応答データに含まれる自端末の情報を暗号化する第2の暗号化手段をさらに備え、前記一括応答手段は、前記配送応答データに含まれる暗号化された情報を復号する第2の復号手段をさらに備えることを特徴とする。

【0018】この発明によれば、各端末は、グループ暗号鍵を受信した場合に自端末の情報を暗号化して中継手段に送信し、中継手段は、各端末からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができる。

【0019】つぎの発明にかかる暗号通信システムは、上記の発明において、前記第1の暗号化手段、前記第2の暗号化手段、前記第1の復号手段、および前記第2の復号手段は、秘密鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする。

【0020】この発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、秘密鍵暗号方式で暗号化され、送受信される。

【0021】つぎの発明にかかる暗号通信システムは、上記の発明において、前記第1の暗号化手段、前記第2の暗号化手段、前記第1の復号手段、および前記第2の復号手段は、公開鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする。

【0022】この発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、公開鍵暗号方式で暗号化され、送受信される。

【0023】つぎの発明にかかる暗号通信システムは、上記の発明において、前記第1の暗号化手段、前記第2の暗号化手段、前記第1の復号手段、および前記第2の復号手段は、既に配送されたグループ暗号鍵を少なくとも保持し、この保持されたグループ暗号鍵のうちの所定のグループ暗号鍵を用いて暗号化または復号を行うことを特徴とする。

【0024】この発明によれば、グループ暗号鍵が更新される場合に、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、使用していたグループ暗号鍵で暗号化され、送受信される。

【0025】つぎの発明にかかる暗号鍵配送方法は、グループ暗号鍵を用いた暗号通信が行われる暗号通信グループを形成する複数の端末が中継手段を介してネットワークに接続され、該ネットワークに接続されたグループ暗号鍵管理手段が前記グループ暗号鍵を生成し、前記中継手段を介して各端末に配送する暗号鍵配送方法において、前記グループ暗号鍵管理手段が、前記グループ暗号鍵を含む鍵配送データを前記端末に一斉に送信する鍵配送データ送信工程と、前記中継手段が、前記鍵配送データに代理応答アドレスとして自中継手段のアドレスを付

加し、該アドレスが付加された鍵配送データを鍵配送終端データとして前記端末に送信する鍵配送終端データ送信工程と、前記端末が、前記鍵配送終端データを受信して前記グループ暗号鍵を受信し、自端末の情報を含む配送応答データを前記中継手段に送信する配送応答データ送信工程と、前記中継手段が、前記端末から受信した配送応答データをもとに、前記グループ暗号鍵を受信した端末の情報を含む一括応答データを前記グループ暗号鍵管理手段に送信する一括応答データ送信工程と、前記グループ暗号鍵管理手段が、前記一括応答データをもとに、前記各端末が前記グループ暗号鍵を受信したか否かを確認する配送結果確認工程と、を含むことを特徴とする。

【0026】この発明によれば、中継手段は、グループ暗号鍵管理手段が送信した鍵配送データに、自中継手段のアドレスを付加して各端末に送信し、各端末は、受信したデータに付加されたアドレスをもとに、自端末の情報を含む配送応答データを中継手段に送信し、中継手段は、端末から受信した配送応答データをもとにグループ暗号鍵を受信した端末の情報をまとめ、一括応答データとしてグループ暗号鍵管理手段に送信する。

【0027】つぎの発明にかかる暗号鍵配送方法は、前記一括応答データ送信工程は、前記一括応答データに含まれる端末の情報を暗号化する第1の暗号化工程をさらに含み、前記配送結果確認工程は、前記一括応答データに含まれる暗号化された端末の情報を復号する第1の復号工程をさらに含むことを特徴とする。

【0028】この発明によれば、中継手段はグループ暗号鍵を受信した端末の情報を暗号化してグループ暗号鍵管理手段に送信し、グループ暗号鍵管理手段は、中継手段からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができる。

【0029】つぎの発明にかかる暗号鍵配送方法は、上記の発明において、前記配送応答データ送信工程は、前記配送応答データに含まれる自端末の情報を暗号化する第2の暗号化工程をさらに含み、前記一括応答データ送信工程は、前記配送応答データに含まれる暗号化された情報を復号する第2の復号工程をさらに含むことを特徴とする。

【0030】この発明によれば、各端末は、グループ暗号鍵を受信した場合に自端末の情報を暗号化して中継手段に送信し、中継手段は、各端末からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができる。

【0031】つぎの発明にかかる暗号鍵配送方法は、上記の発明において、前記第1の暗号化工程、前記第2の暗号化工程、前記第1の復号工程、および前記第2の復号工程は、秘密鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする。

【0032】この発明によれば、一括応答データに含ま

れる端末の情報、および配送応答データに含まれる自端末の情報は、秘密鍵暗号方式で暗号化され、送受信される。

【0033】つぎの発明にかかる暗号鍵配送方法は、上記の発明において、前記第1の暗号化工程、前記第2の暗号化工程、前記第1の復号工程、および前記第2の復号工程は、公開鍵暗号方式によってそれぞれ暗号化または復号を行うことを特徴とする。

【0034】この発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、公開鍵暗号方式で暗号化され、送受信される。

【0035】つぎの発明にかかる暗号鍵配送方法は、上記の発明において、前記第1の暗号化工程、前記第2の暗号化工程、前記第1の復号工程、および前記第2の復号工程は、既に配送されたグループ暗号鍵を少なくとも保持し、この保持されたグループ暗号鍵のうちの所定のグループ暗号鍵を用いて暗号化または復号を行うことを特徴とする。

【0036】この発明によれば、グループ暗号鍵が更新される場合に、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、使用していたグループ暗号鍵で暗号化され、送受信される。

【0037】

【発明の実施の形態】以下に添付図面を参照して、この発明に係る暗号通信システムおよび暗号鍵配送方法の好適な実施の形態を詳細に説明する。

【0038】実施の形態1。図1は、この発明の第1の実施の形態である暗号通信システムの構成を示す図である。図1において、暗号通信システムは、グループ暗号鍵管理部1、中継手段としての機能を有するルータ5、8が、ネットワーク4に接続されている。ルータ5はさらにLAN11を介して端末T1～T4に接続される。また、ルータ8は、LAN12を介して端末T5～T7と接続されている。さらに、端末T2～T6は、暗号通信グループ13に含まれている。なお、ネットワーク4は、電話網や、ISDN網などを含んでもよい。

【0039】グループ暗号鍵管理部1は、暗号通信グループ13が暗号通信に用いるグループ暗号鍵を生成する。グループ暗号鍵管理部1は、生成したグループ暗号鍵を含む鍵配送データD1を暗号通信グループに属する各端末T2～T6にマルチキャスト送信する鍵配送部2と、一括応答データD4をもとに暗号通信グループに属する各端末T2～T6の情報を管理するグループ端末管理部3を有している。

【0040】ルータ5はグループ暗号鍵管理部1が送信した鍵配送データD1に、代理応答アドレスとしてルータ5のIPアドレスを付加して鍵配送終端データD2を作成するアドレス付加部6を有し、LAN11に接続された端末T1～T4に鍵配送終端データD2を送信す

る。また、ルータ5は、暗号通信グループ13に属する端末T2～T4がグループ暗号鍵を受信した場合に送出する配送応答データD3をもとに、グループ暗号鍵を受信した端末の情報を暗号化し、グループ暗号鍵管理部1に一括応答データD4として送信する一括応答部7を有する。

【0041】また、ルータ8は、ルータ5と同様に、グループ暗号鍵管理部1が送信した鍵配送データD1に、代理応答アドレスとしてルータ8のIPアドレスを付加して鍵配送終端データD2を作成するアドレス付加部9を有し、LAN12に接続された端末T5～T7に鍵配送終端データD2を送信する。さらに、ルータ8は、暗号通信グループ13に属する端末T5～T6がグループ暗号鍵を受信した場合に送出する配送応答データD3をもとに、グループ暗号鍵を受信した端末の情報を暗号化し、グループ暗号鍵管理部1に一括応答データD4として送信する一括応答部10を有する。

【0042】端末T2は、鍵配送終端データD2を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データD3としてルータ5に送信する暗号鍵管理部t2を有する。端末T3、T4は、端末T2と同様に鍵配送終端データD2を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データD3としてルータ5に送信する暗号鍵管理部t3、t4を有する。なお、端末T1は、LAN11に接続されているが、暗号通信グループ13には属さない。

【0043】端末T5、T6は、鍵配送終端データD2を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データD3としてルータ8に送信する暗号鍵管理部t5、t6を有する。なお、端末T7は、LAN11に接続されているが、暗号通信グループ13には属さない。

【0044】さらに、グループ暗号鍵管理部1の鍵配送部2とグループ端末管理部3、ルータ5の一括応答部7、ルータ8の一括応答部10および端末T2～T6の暗号鍵管理部t2～t6は、秘密鍵暗号に用いる暗号鍵KCCを共有している。秘密鍵暗号にはたとえば米国の標準暗号方式DES(Data Encryption Standard)などがあるが、暗号鍵を知らない者が暗号文から平文を推定できないようなものならいかなる方式でもよい。

【0045】ここで、図2を参照して、鍵配送データD1、鍵配送終端データD2、配送応答データD3、一括応答データD4についてさらに詳細に説明する。

【0046】鍵配送データD1は、グループ暗号鍵管理部1の鍵配送部2によって作成される。鍵配送データD1は、送信元IPアドレス、宛先IPアドレス、データ種別、グループ識別子、グループ暗号鍵データを有する。鍵配送部2は、鍵配送データD1の送信元IPアドレスにグループ暗号鍵管理部1のIPアドレスを設定し、宛先IPアドレスには暗号通信グループ13のマル

チキャストアドレスを設定し、データ種別には鍵配送を設定し、グループ識別子には暗号通信グループ13を識別するID13を設定し、グループ暗号鍵データにグループ暗号鍵管理部1が作成したグループ暗号鍵KSEを設定する。さらに、グループ識別子およびグループ暗号鍵を、暗号鍵KCCで暗号化している。

【0047】鍵配送終端データD2は、鍵配送データD1をもとに、ルータのアドレス付加部によって作成される。鍵配送終端データD2は、送信元IPアドレス、宛先IPアドレス、データ種別、グループ識別子、グループ暗号鍵データ、代理応答アドレス、を有する。鍵配送終端データD2には、ルータのアドレス付加部が鍵配送データD1に代理応答アドレスとして自己のIPアドレスを付加している。すなわち、ルータ5のアドレス付加部6は、代理応答アドレスとしてルータ5のIPアドレスを付加し、ルータ8のアドレス付加部9は、代理応答アドレスとしてルータ8のIPアドレスを付加する。また、鍵配送終端データD2の、送信元IPアドレス、宛先IPアドレス、暗号化されたグループ識別子およびグループ暗号鍵データは、鍵配送データD1から変更されず、データ種別は、鍵配送から鍵配送終端に書き替えられる。

【0048】配送応答データD3は、鍵配送終端データD2をもとに、端末の暗号鍵管理部によって作成される。配送応答データD3は、送信元IPアドレス、宛先IPアドレス、データ種別、グループ識別子、配送済み端末IPアドレス、を有する。端末の暗号鍵管理部は、鍵配送終端データD2を受信し、暗号化されたグループ識別子およびグループ暗号鍵データを暗号鍵KCCで復号し、グループ暗号鍵KSEを取り出し、グループ暗号鍵を正常に受信したことを示す配送応答データD3を作成する。具体的には、送信元IPアドレスに自端末のIPアドレスを設定し、宛先アドレスに鍵配送終端データD2の代理応答アドレスに設定されたルータのIPアドレスを設定し、データ種別に配送応答を設定し、グループ識別子に暗号通信グループ13を識別するID13を設定し、配送済み端末IPアドレスに自端末のIPアドレスを設定する。さらに、グループ識別子および配送済み端末IPアドレスは暗号鍵KCCで暗号化される。

【0049】すなわち、端末T2の暗号鍵管理部t2は、送信元IPアドレスおよび配送済み端末IPアドレスに端末T2のIPアドレスを設定し、宛先IPアドレスにはルータ5のIPアドレスを設定する。また、端末T3およびT4の暗号鍵管理部t3およびt4も同様に送信元IPアドレスおよび配送済み端末IPアドレスに自端末のIPアドレスを設定し、宛先IPアドレスにルータ5のIPアドレスを設定する。さらに、端末T5およびT6においても同様である。端末T5およびT6では、鍵配送終端データD2はルータ8から受信しており、代理応答アドレスはルータ8のIPアドレスである

ため、宛先IPアドレスはルータ8のIPアドレスとなる。また、端末T1および端末T7は、暗号通信グループ13に属さず、受信した鍵配送終端データD2を破棄する。

05 【0050】一括応答データD4は、各端末から受信した配送応答データD3をもとに、ルータの一括応答部によって作成される。一括応答データD4は、送信元IPアドレス、宛先IPアドレス、データ種別、グループ識別子、配送済み有効数、配送済み端末複数IPアドレスを有する。ルータの一括応答部は、ルータが鍵配送終端データD2を送信してから一定時間内に受信した配送応答データD3のグループ識別子および配送済み端末IPアドレスを暗号鍵KCCで復号し、グループ暗号鍵を正常に受信した端末の数と、各端末のIPアドレスとを得る。さらに一括応答部は、送信元IPアドレスに自ルータのIPアドレスを設定し、宛先IPアドレスにグループ鍵管理部1のIPアドレスを設定し、データ種別に一括応答を設定し、グループ識別子に暗号通信グループ13を識別するID13を設定し、配送済み有効数にグループ暗号鍵を正常に受信した端末の数を設定し、配送済み端末複数IPアドレスにグループ暗号鍵を正常に受信した各端末のIPアドレスを設定する。さらに、グループ識別子、配送済み有効数、配送済み端末複数IPアドレスを暗号鍵KCCで暗号化する。

25 【0051】具体的には、ルータ5の一括応答部7は、端末T2、端末T3、端末T4からそれぞれ配送応答データD3を受信し、各配送応答データD3の暗号化されたグループ識別子および配送済み端末IPアドレスを暗号鍵KCCで復号し、端末T2、端末T3、端末T4のIPアドレスを得る。さらに一括応答部7は、送信元IPアドレスにルータ5のIPアドレスを設定し、宛先IPアドレスにグループ暗号鍵管理部1のIPアドレスを設定し、データ種別に一括応答を設定し、グループ識別子に暗号通信グループ13を識別するID13を設定し、配送済み有効数に3を設定し、配送済み端末複数IPアドレスに端末T2、T3、T4のIPアドレスをそれぞれ設定し、グループ識別子、配送済み有効数、配送済み端末複数IPアドレスを暗号鍵KCCで暗号化する。

40 【0052】また、ルータ8の一括応答部10は、端末T5およびT6からそれぞれ配送応答データD3を受信し、各配送応答データD3の暗号化されたグループ識別子および配送済み端末IPアドレスを暗号鍵KCCで復号し、端末T5および端末T6のIPアドレスを得る。さらに一括応答部10は、送信元IPアドレスにルータ8のIPアドレスを設定し、宛先IPアドレスにグループ暗号鍵管理部1のIPアドレスを設定し、データ種別に一括応答を設定し、グループ識別子に暗号通信グループ13を識別するID13を設定し、配送済み有効数に2を設定し、配送済み端末複数IPアドレスに端末T5



およびT6のIPアドレスを設定し、グループ識別子、配送済み有効数、配送済み端末複数IPアドレスを暗号鍵KCCで暗号化する。

【0053】つぎに、図3に示すタイミングシーケンスを参照して、グループ暗号鍵の配送についてさらに説明する。

【0054】まず、グループ暗号鍵管理部1は、グループ暗号鍵KSEを生成する。鍵配送部2は、暗号鍵KCCでグループ暗号鍵KSEを暗号化してKCC(KSE)を作成し、  
グループ暗号鍵管理部1:  $KCC(KSE) = ENC(KSE, KCC)$   
鍵配送データD1として各端末にマルチキャスト送信する。

【0055】ルータ5は、鍵配送データD1を受信し、代理応答アドレスとしてルータ5のIPアドレスを付加し、鍵配送終端データD2としてLAN11に接続された端末T1～T4に配送する。データD2には、暗号鍵KCCで暗号化されたグループ鍵暗号、KCC(KSE)が含まれる。

【0056】ルータ8は、鍵配送データD1を受信し、代理応答アドレスとしてルータ8のIPアドレスを付加し、鍵配送終端データD2としてLAN12に接続された端末T5～T7に配送する。鍵配送終端データD2には、暗号鍵KCCで暗号化されたグループ鍵暗号、KCC(KSE)が含まれる。

【0057】端末T1は、鍵配送終端データD2を受信するが、暗号通信グループ13に属さず、暗号鍵KCCを有さないので、鍵配送終端データD2に含まれるKCC(KSE)を復号することはできない。

【0058】端末T2は、鍵配送終端データD2を受信し、暗号鍵KCCを用いてKCC(KSE)を復号し、グループ暗号鍵KSEを得る。

端末T2:  $KSE = DEC(KCC(KSE), KC)$

さらに、端末T2は、端末T2のIPアドレスであるIP(T2)を暗号鍵KCCで暗号化してKCC(IP(T2))を作成し、

端末T2:  $KCC(IP(T2)) = ENC(IP(T2), KCC)$

グループ暗号鍵KSEを受信したことを伝える配送応答データD3を作成し、ルータ5に送信する。

【0059】端末T3およびT4は、端末T2と同様に、鍵配送終端データD2を受信し、暗号鍵KCCを用いてKCC(KSE)を復号してグループ暗号鍵KSEを得る。

端末T3:  $KSE = DEC(KCC(KSE), KC)$

端末T4:  $KSE = DEC(KCC(KSE), KC)$

また、端末T3およびT4は、各端末のIPアドレスを暗号鍵KCCで暗号化する。

端末T3:  $KCC(IP(T3)) = ENC(IP(T3), KCC)$

50 端末T4:  $KCC(IP(T4)) = ENC(IP(T4), KCC)$

グループ暗号鍵KSEを受信したことを伝える配送応答データD3を作成し、ルータ5に送信する。

【0060】端末T5およびT6は、端末T2～T4と同様に、鍵配送終端データD2を受信し、暗号鍵KCCを用いてKCC(KSE)を復号してグループ暗号鍵KSEを得る。

端末T5:  $KSE = DEC(KCC(KSE), KC)$

15 端末T6:  $KSE = DEC(KCC(KSE), KC)$

また、端末T5およびT6は、各端末のIPアドレスを暗号鍵KCCで暗号化し、

20 端末T5:  $KCC(IP(T5)) = ENC(IP(T5), KCC)$

端末T6:  $KCC(IP(T6)) = ENC(IP(T6), KCC)$

グループ暗号鍵KSEを受信したことを伝える配送応答データD3を作成し、ルータ8に送信する。

25 【0061】端末T7は、鍵配送終端データD2を受信するが、暗号通信グループ13に属さず、暗号鍵KCCを有さないので、鍵配送終端データD2に含まれるKCC(KSE)を復号することはできない。

【0062】ルータ5は、端末T2～T4から配送応答データD3を受け取り、暗号鍵KCCで復号し、各端末のIPアドレス、IP(T2)、IP(T3)、IP(T4)を得る。

ルータ5:  $IP(T2) = DEC(KCC(IP(T2)), KCC)$

35  $IP(T3) = DEC(KCC(IP(T3)), KC)$

$IP(T4) = DEC(KCC(IP(T4)), KC)$

さらにルータ5は、受信したIPアドレスの数3と、各端末のIPアドレス、IP(T2)、IP(T3)、IP(T4)を、暗号鍵KCCで暗号化し、一括応答データD4としてグループ暗号鍵管理部1に送信する。

【0063】ルータ8は、端末T5およびT6から配送応答データD3を受け取り、暗号鍵KCCで復号し、各

45 端末のIPアドレス、IP(T5)、IP(T6)を得る。

ルータ8:  $IP(T5) = DEC(KCC(IP(T5)), KCC)$

50  $IP(T6) = DEC(KCC(IP(T6)), KC)$

さらにルータ8は、受信したIPアドレスの数2と、各端末のIPアドレス、IP(T5)、IP(T6)を暗号鍵KCCで暗号化し、一括応答データD4としてグループ暗号鍵管理部1に送信する。

【0064】グループ暗号鍵管理部1はルータ5およびルータ8から受信した一括応答データD4を暗号鍵KCCで復号し、グループ暗号鍵KSEを受信した端末T2～T6のIPアドレスを得ることができる。

【0065】このようにして、グループ暗号鍵KSEは、暗号通信グループ13に属する各端末に共有される。したがって、暗号通信グループ13に属する端末、たとえば端末T6が、グループ暗号鍵KSEを用いて秘密鍵暗号方式で通信データを暗号化し、暗号通信グループ13に属する端末にマルチキャスト送信した場合には、端末T2～T5は、グループ暗号鍵KSEで受信したデータを復号することができる。

【0066】この実施の形態1では、グループ暗号鍵KSEが配送された場合に、暗号通信グループ13に属する端末T2～T6は、グループ暗号鍵管理部1に直接配送応答をするのではなく、各端末からルータに配送応答をし、ルータが端末の配送応答データをまとめ、一括してグループ暗号鍵管理部1に配送応答をする。したがって、直接各端末からグループ暗号鍵管理部に配送応答をする場合に比べてネットワーク4に送信される通信量は減少し、ネットワークの負荷を少なくすることができる。

【0067】また、この実施の形態1では、グループ暗号鍵管理部1と、ルータ5および8と、端末T2～T6と、で暗号鍵KCCを共有し、グループ暗号鍵KSEの配送応答および一括応答を秘密鍵暗号方式で暗号化している。したがって、グループ暗号鍵の配送応答のセキュリティを高めることができる。

【0068】なお、この実施の形態1では、配送応答データD3および一括応答データD4に配送済み端末IPアドレスを有していたが、必ずしもIPアドレスである必要はなく、グループ暗号鍵管理部で端末を識別する固有の番号でもよい。たとえば、IPアドレスのかわりに、MACアドレスや、端末の製造番号を用いても同様の効果を奏することができる。

【0069】また、この実施の形態1では、グループ暗号鍵KSEの配送、配送応答、一括応答のすべてに同一の暗号鍵KCCを用いて暗号化を行っているが、それぞれ異なる暗号鍵を用いて暗号化するようにしてもよいし、ネットワークやLANのセキュリティの状況によっては、とくに暗号化を行わなくてもよい。

【0070】実施の形態2。つぎに、この発明の実施の形態2について説明する。この実施の形態2では、グループ暗号鍵を受信した端末は、自端末の情報を公開鍵暗号方式で暗号化してルータに送信し、ルータは端末から受信した情報を復号し、一括してグループ暗号鍵管理部

に送信している。

【0071】図4は、この発明の実施の形態2である暗号通信システムの構成を示す図である。図4において暗号通信システムは、実施の形態1に示した暗号通信システムと同様に、グループ暗号鍵管理部40、中継手段としての機能を有するルータ42およびルータ44が、ネットワーク4に接続されている。ルータ42はさらにLAN11を介して端末T1～T4と接続されている。また、ルータ44は、LAN12を介して端末T5～T7と接続されている。さらに、端末T2～T6は、暗号通信グループ13に含まれている。

【0072】グループ暗号鍵管理部40は、暗号通信グループ13が暗号通信に用いるグループ暗号鍵を生成する。グループ暗号鍵管理部40は、生成したグループ暗号鍵を含む鍵配送データD1を暗号通信グループに属する各端末にマルチキャスト送信する鍵配送部2と、一括応答データD6をもとに暗号通信グループに属する各端末の情報を管理するグループ端末管理部41を有している。

【0073】ルータ42は、グループ暗号鍵管理部40が送信した鍵配送データD1に、代理応答アドレスとしてルータ42のIPアドレスを付加して鍵配送終端データD2を作成するアドレス付加部6を有し、LAN11に接続された端末T1～T4に鍵配送終端データD2を送信する。また、ルータ42は、暗号通信グループ13に属する端末T2～T4がグループ暗号鍵を受信した場合に送出する配送応答データD5をもとに、グループ暗号鍵を受信した端末の情報を暗号化し、グループ暗号鍵管理部1に一括応答データD6として送信する一括応答部43を有する。

【0074】また、ルータ44もルータ42と同様に、グループ暗号鍵管理部40が送信した鍵配送データD1に、代理応答アドレスとしてルータ44のIPアドレスを付加して鍵配送終端データD2を作成するアドレス付加部9を有し、LAN12に接続された端末T5～T7に鍵配送終端データD2を送信する。さらに、ルータ44は、暗号通信グループ13に属する端末T5およびT6がグループ暗号鍵を受信した場合に送出する配送応答データD5をもとに、グループ暗号鍵を受信した端末の情報を暗号化し、グループ暗号鍵管理部40に一括応答データD6として送信する一括応答部45を有する。

【0075】端末T2は、鍵配送終端データD2を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データD5としてルータ42に送信する暗号鍵管理部42を有する。端末T3、T4は、同様に鍵配送終端データD2を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データD5としてルータ42に送信する暗号鍵管理部43、44を有する。

【0076】端末T5、T6は、鍵配送終端データD2

を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データD5としてルータ44に送信する暗号鍵管理部t45、t46を有する。

【0077】さらに、グループ暗号鍵管理部40の鍵配送部2、および端末T2～T6の暗号鍵管理部t42～t46は、秘密鍵暗号に用いる暗号鍵KCCを共有している。秘密鍵暗号にはたとえば米国の標準暗号方式DES (Data Encryption Standard) などがあるが、暗号鍵を知らない者が暗号文から平文を推定できないようなものならいかなる方式でもよい。

【0078】また、ルータ42の一括応答部43は、公開鍵暗号に用いる秘密鍵KS42を保持しており、端末T2～T4の暗号鍵管理部t42～t44は、秘密鍵KS42に対応する公開鍵KP42を保持している。同様に、ルータ44の一括応答部45は、公開鍵暗号に用いる秘密鍵KS44を保持しており、端末T5～T6の暗号鍵管理部t45～t46は、秘密鍵KS44に対応する公開鍵KP44を保持している。

【0079】さらに、グループ暗号鍵管理部40のグループ端末管理部41は、公開鍵暗号に用いる秘密鍵KS40を保持しており、ルータ42の一括応答部43およびルータ44の一括応答部45は、秘密鍵KS40に対応する公開鍵KP40を保持している。公開鍵暗号としては、RSA (Rivest Shamir Adleman) 暗号や、楕円Elgamal暗号などを用いることができる。

【0080】つぎに、鍵配送データD1、鍵配送終端データD2、配送応答データD5、一括応答データD6について説明する。鍵配送データD1および鍵配送終端データD2については、実施の形態1に示した鍵配送データおよび鍵配送終端データと同様である。

【0081】配送応答データD5は、実施の形態1に示した配送応答データD3に対応し、公開鍵暗号方式でグループ識別子および配送済み端末IPアドレスを暗号化する。すなわち、端末T2～T4の暗号鍵管理部t42～t44は、ルータ42に対応し、公開鍵KP42を用いて暗号化を行う。また、端末T5およびT6の暗号鍵管理部t45およびt46は、ルータ44に対応し、公開鍵KP44を用いて暗号化を行う。

【0082】一括応答データD6は、実施の形態1に示した一括応答データD4に対応し、公開鍵暗号方式でグループ識別子、配送済み有効数、配送済み端末複数IPアドレスを暗号化する。すなわち、ルータ42およびルータ44は、公開鍵KP40を用いて暗号化を行う。

【0083】つぎに、図5に示すタイミングシーケンスを参照して、グループ暗号鍵の配送についてさらに説明する。

【0084】まず、グループ暗号鍵管理部40は、グループ暗号鍵KSEを生成する。鍵配送部2は、暗号鍵KCCでグループ暗号鍵KSEを暗号化してKCC (KSE) を作成し、グループ暗号鍵管理部40 : KCC (K

SE) = ENC (KSE, KCC) 鍵配送データD1として各端末にマルチキャスト送信する。

【0085】ルータ42は、鍵配送データD1を受信し、代理応答アドレスとしてルータ42のIPアドレスを付加し、鍵配送終端データD2としてLAN11に接続された端末T1～T4に配送する。データD2には、暗号鍵KCCで暗号化されたグループ暗号鍵、KCC (KSE) が含まれる。

【0086】ルータ44は、鍵配送データD1を受信し、代理応答アドレスとしてルータ44のIPアドレスを付加し、鍵配送終端データD2としてLAN12に接続された端末T5～T7に配送する。鍵配送終端データD2には、暗号鍵KCCで暗号化されたグループ暗号鍵、KCC (KSE) が含まれる。

【0087】端末T1は、鍵配送終端データD2を受信するが、暗号通信グループ13に属さず、暗号鍵KCCを有さないため、鍵配送終端データD2に含まれるKCC (KSE) を復号することはできない。

【0088】端末T2は、鍵配送終端データD2を受信し、暗号鍵KCCを用いてKCC (KSE) を復号し、グループ暗号鍵KSEを得る。

端末T2 :  $KSE = DEC (KCC (KSE), KCC)$   
さらに、端末T2は、端末T2のIPアドレスであるIP (T2) を公開鍵KP42で暗号化してKP42 (IP (T2)) を作成し、

端末T2 :  $KP42 (IP (T2)) = ENC (IP (T2), KP42)$   
グループ暗号鍵KSEを受信したことを伝える配送応答データD5を作成し、ルータ42に送信する。

【0089】端末T3およびT4も、端末T2と同様に、鍵配送終端データD2を受信し、暗号鍵KCCを用いてKCC (KSE) を復号してグループ暗号鍵KSEを得る。

端末T3 :  $KSE = DEC (KCC (KSE), KCC)$   
端末T4 :  $KSE = DEC (KCC (KSE), KCC)$

また、端末T3およびT4は、各端末のIPアドレスを公開鍵KP42で暗号化し、

端末T3 :  $KP42 (IP (T3)) = ENC (IP (T3), KP42)$   
端末T4 :  $KP42 (IP (T4)) = ENC (IP (T4), KP42)$

グループ暗号鍵KSEを受信したことを伝える配送応答データD5を作成し、ルータ42に送信する。

【0090】端末T5およびT6も、端末T2～T4と同様に、鍵配送終端データD2を受信し、暗号鍵KCCを用いてKCC (KSE) を復号してグループ暗号鍵KSEを得る。

端末T5:  $KSE = DEC(KCC(KSE), KC)$   
C)

端末T6:  $KSE = DEC(KCC(KSE), KC)$   
C)

また、端末T5およびT6は、各端末のIPアドレスを公開鍵KP44で暗号化し、

端末T5:  $KP44(IP(T5)) = ENC(IP(T5), KP44)$

端末T6:  $KP44(IP(T6)) = ENC(IP(T6), KP44)$

グループ暗号鍵KSEを受信したことを伝える配送応答データD5を作成し、ルータ44に送信する。

【0091】端末T7は、鍵配送終端データD2を受信するが、暗号通信グループ13に属さず、暗号鍵KCCを有さないのので、鍵配送終端データD2に含まれるKCC(KSE)を復号することはできない。

【0092】ルータ42は、端末T2～T4から配送応答データD5を受け取り、秘密鍵KS42で復号し、各端末のIPアドレス、IP(T2)、IP(T3)、IP(T4)を得る。

ルータ42:  $IP(T2) = DEC(KP42(IP(T2)), KS42)$

$IP(T3) = DEC(KP42(IP(T3)), KS42)$

$IP(T4) = DEC(KP42(IP(T4)), KS42)$

さらにルータ42は、受信したIPアドレスの数3と、各端末のIPアドレス、IP(T2)、IP(T3)、IP(T4)を、公開鍵KP40で暗号化し、一括応答データD6としてグループ暗号鍵管理部40に送信する。

【0093】ルータ44は、端末T5～T6から配送応答データD5を受け取り、秘密鍵KS44で復号し、各端末のIPアドレス、IP(T5)、IP(T6)を得る。

ルータ44:  $IP(T5) = DEC(KP44(IP(T5)), KS44)$

$IP(T6) = DEC(KP44(IP(T6)), KS44)$

さらにルータ44は、受信したIPアドレスの数2と、各端末のIPアドレス、IP(T5)、IP(T6)を公開鍵KP40で暗号化し、一括応答データD6としてグループ暗号鍵管理部40に送信する。

【0094】グループ暗号鍵管理部40はルータ42およびルータ44から受信した一括応答データD6を秘密鍵KS40で復号し、グループ暗号鍵KSEを受信した端末T2～T6のIPアドレスを得ることができる。

【0095】このようにして、グループ暗号鍵KSEは、暗号通信グループ13に属する各端末に共有される。したがって、暗号通信グループ13に属する端末、

たとえば端末T6が、グループ暗号鍵KSEを用いて秘密鍵暗号方式で通信データを暗号化し、暗号通信グループ13に属する端末にマルチキャスト送信した場合には、端末T2～T5は、グループ暗号鍵KSEで受信したデータを復号することができる。

【0096】この実施の形態2では、グループ暗号鍵KSEが配送された場合に、暗号通信グループ13に属する端末T2～T6は、グループ暗号鍵管理部40に直接配送応答をするのではなく、各端末からルータに配送応答をし、ルータが端末の配送応答データをまとめ、一括してグループ暗号鍵管理部40に配送応答をする。したがって、直接各端末からグループ暗号鍵管理部に配送応答をする場合に比べてネットワーク4に送信される通信量は減少し、ネットワークの負荷を少なくすることができる。

【0097】また、この実施の形態2では、グループ暗号鍵KSEの配送応答および一括応答を公開鍵暗号方式で暗号化している。したがって、グループ暗号鍵の配送応答のセキュリティをより高めることができる。

【0098】なお、この実施の形態2では、配送応答データD5および一括応答データD6に配送済み端末IPアドレスを有していたが、必ずしもIPアドレスである必要はなく、グループ暗号鍵管理部で端末を識別する固有の番号でもよい。たとえば、IPアドレスのかわりに、MACアドレスや、端末の製造番号を用いても同様の効果を奏することができる。

【0099】実施の形態3. つぎに、この発明の実施の形態3について説明する。この実施の形態3では、暗号通信グループに属する各端末は、すでにグループ暗号鍵KSEN0を共有している。暗号鍵管理部60は、新規のグループ暗号鍵KSEN1を生成し、暗号通信グループに属する各端末に配送し、グループ暗号鍵を更新する。また、新規のグループ暗号鍵の配送、配送応答、一括応答は、既に共有されているグループ暗号鍵KSEN0で暗号化される。

【0100】図6は、この発明の実施の形態3である暗号通信システムの構成を示す図である。図6において暗号通信システムは、実施の形態1に示した暗号通信システムと同様に、グループ暗号鍵管理部60、中継手段としての機能を有するルータ63およびルータ66が、ネットワーク4に接続されている。ルータ63はさらにLAN11を介して端末T1、端末T2、端末T3および端末T4と接続されている。また、ルータ66は、LAN12を介して端末T5、端末T6および端末T7と接続されている。さらに、端末T2～T6は、暗号通信グループ13に含まれている。

【0101】グループ暗号鍵管理部60は、暗号通信グループ13が暗号通信に用いるグループ暗号鍵を生成する。グループ暗号鍵管理部60は、生成したグループ暗号鍵を含む鍵配送データD61を暗号通信グループに属

する各端末にマルチキャスト送信する鍵配送部61と、一括応答データD64をもとに暗号通信グループに属する各端末の情報を管理するグループ端末管理部62を有している。

【0102】ルータ63は、グループ暗号鍵管理部60が送信した鍵配送データD61に、代理応答アドレスとしてルータ63のIPアドレスを付加して鍵配送終端データD62を作成するアドレス付加部64を有し、LAN11に接続された端末T1～T4に鍵配送終端データD62を送信する。また、ルータ63は、暗号通信グループ13に属する端末T2～T4がグループ暗号鍵を受信した場合に送出する配送応答データD63をもとに、グループ暗号鍵を受信した端末の情報を暗号化し、グループ暗号鍵管理部60に一括応答データD64として送信する一括応答部65を有する。

【0103】また、ルータ66は、ルータ63と同様に、グループ暗号鍵管理部60が送信した鍵配送データD61に、代理応答アドレスとしてルータ66のIPアドレスを付加して鍵配送終端データD62を作成するアドレス付加部67を有し、LAN12に接続された端末T5～T7に鍵配送終端データD62を送信する。さらに、ルータ66は、暗号通信グループ13に属する端末T5～T6がグループ暗号鍵を受信した場合に送出する配送応答データD63をもとに、グループ暗号鍵を受信した端末の情報を暗号化し、グループ暗号鍵管理部60に一括応答データD64として送信する一括応答部68を有する。

【0104】端末T2は、鍵配送終端データD62を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データD63としてルータ63に送信する暗号鍵管理部t62を有する。端末T3、T4は、同様に鍵配送終端データD62を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データD63としてルータ63に送信する暗号鍵管理部t63、t64を有する。

【0105】端末T5、T6は、鍵配送終端データD62を受信してグループ暗号鍵を受信し、自端末の情報を暗号化し、配送応答データD63としてルータ66に送信する暗号鍵管理部t65、t66を有する。

【0106】さらに、グループ暗号鍵管理部60の鍵配送部61、ルータ63、66、および端末T2～T6の暗号鍵管理部t62～t66は、グループ暗号鍵KSEN0を共有している。

【0107】つぎに、鍵配送データD61、鍵配送終端データD62、配送応答データD63、一括応答データD64について説明する。

【0108】鍵配送データD61は、実施の形態1に示した鍵配送データD1に対応し、既に共有されているグループ暗号鍵KSEN0でグループ識別子および配送済み端末のIPアドレスを暗号化される。

【0109】鍵配送終端データD62は、実施の形態1に示した鍵配送終端データD2に対応している。

【0110】配送応答データD63は、実施の形態1に示した配送応答データD3に対応し、既に共有されているグループ暗号鍵KSEN0でグループ識別子および配送済み端末IPアドレスを暗号化される。

【0111】一括応答データD64は、実施の形態1に示した一括応答データD4に対応し、既に共有されているグループ暗号鍵KSEN0でグループ識別子、配送済み有効数、配送済み端末複数IPアドレスを暗号化される。

【0112】つぎに、図7に示すタイミングシーケンスを参照して、グループ暗号鍵の配送についてさらに説明する。

【0113】まず、グループ暗号鍵管理部60、ルータ63、66、端末T2～T6は、なんらかの手段でグループ暗号鍵KSEN0をすでに共有している。グループ暗号鍵管理部60は、新規のグループ暗号鍵KSEN1を生成する。鍵配送部61は、グループ暗号鍵KSEN0で新規のグループ暗号鍵KSEN1を暗号化してKSEN0 (KSEN1)を作成し、グループ暗号鍵管理部60:KSEN0 (KSEN1)=ENC (KSEN1, KSEN0) 鍵配送データD61として各端末にマルチキャスト送信する。

【0114】ルータ63は、鍵配送データD61を受信し、代理応答アドレスとしてルータ63のIPアドレスを付加し、鍵配送終端データD62としてLAN11に接続された端末T1～T4に配送する。鍵配送終端データD62には、グループ暗号鍵KSEN0で暗号化された新規のグループ暗号鍵、KSEN0 (KSEN1)が含まれる。

【0115】ルータ66は、鍵配送データD61を受信し、代理応答アドレスとしてルータ66のIPアドレスを付加し、鍵配送終端データD62としてLAN12に接続された端末T5～T7に配送する。鍵配送終端データD62には、グループ暗号鍵KSEN0で暗号化された新規のグループ暗号鍵、KSEN0 (KSEN1)が含まれる。

【0116】端末T2は、鍵配送終端データD62を受信し、グループ暗号鍵KSEN0を用いてKSEN0 (KSEN1)を復号し、新規のグループ暗号鍵KSEN1を得る。

端末T2:KSEN1=DEC (KSEN0 (KSEN1), KSEN0)

さらに、端末T2は、端末T2のIPアドレスであるIP (T2)をグループ暗号鍵KSEN0で暗号化してKSEN0 (IP (T2))を作成し、

端末T2:KSEN0 (IP (T2))=ENC (IP (T2), KSEN0)

新規のグループ暗号鍵KSEN1を受信したことを伝え

る配送応答データD63を作成し、ルータ63に送信する。

【0117】端末T3およびT4は、端末T2と同様に、鍵配送終端データD62を受信し、グループ暗号鍵KSEN0を用いてKSEN0(KSEN1)を復号し、新規のグループ暗号鍵KSEN1を得る。

端末T3:  $KSEN1 = DEC(KSEN0(KSEN1), KSEN0)$

端末T4:  $KSEN1 = DEC(KSEN0(KSEN1), KSEN0)$

また、端末T3およびT4は、各端末のIPアドレスをグループ暗号鍵KSEN0で暗号化し、

端末T3:  $KSEN0(IP(T3)) = ENC(IP(T3), KSEN0)$

端末T4:  $KSEN0(IP(T4)) = ENC(IP(T4), KSEN0)$

新規のグループ暗号鍵KSEN1を受信したことを伝える配送応答データD63を作成し、ルータ63に送信する。

【0118】端末T5およびT6は、端末T2~T4と同様に、鍵配送終端データD62を受信し、グループ暗号鍵KSEN0を用いてKSEN0(KSEN1)を復号して新規のグループ暗号鍵KSEN1を得る。

端末T5:  $KSEN1 = DEC(KSEN0(KSEN1), KSEN0)$

端末T6:  $KSEN1 = DEC(KSEN0(KSEN1), KSEN0)$

また、端末T5およびT6は、各端末のIPアドレスをグループ暗号鍵KSEN0で暗号化し、

端末T5:  $KSEN0(IP(T5)) = ENC(IP(T5), KSEN0)$

端末T6:  $KSEN0(IP(T6)) = ENC(IP(T6), KSEN0)$

新規のグループ暗号鍵KSEN1を受信したことを伝える配送応答データD63を作成し、ルータ66に送信する。

【0119】端末T7は、鍵配送終端データD62を受信するが、暗号通信グループ13に属さず、グループ暗号鍵KSEN0を有さないの、鍵配送終端データD62に含まれるKSEN0(KSEN1)を復号することはできない。

【0120】ルータ63は、端末T2~T4から配送応答データD63を受け取り、グループ暗号鍵KSEN0で復号し、各端末のIPアドレス、IP(T2)、IP(T3)、IP(T4)を得る。

ルータ63:  $IP(T2) = DEC(KSEN0(IP(T2)), KSEN0)$

$IP(T3) = DEC(KSEN0(IP(T3)), KSEN0)$

$IP(T4) = DEC(KSEN0(IP(T4)),$

$KSEN0)$

さらにルータ63は、受信したIPアドレスの数3と、各端末のIPアドレス、IP(T2)、IP(T3)、IP(T4)を、グループ暗号鍵KSEN0で暗号化し、一括応答データD64としてグループ暗号鍵管理部60に送信する。

【0121】ルータ66は、端末T5~T6から配送応答データD63を受け取り、グループ暗号鍵KSEN0で復号し、各端末のIPアドレス、IP(T5)、IP(T6)を得る。

ルータ66:  $IP(T5) = DEC(KSEN0(IP(T5)), KSEN0)$

$IP(T6) = DEC(KSEN0(IP(T6)), KSEN0)$

さらにルータ66は、受信したIPアドレスの数2と、各端末のIPアドレス、IP(T5)、IP(T6)をグループ暗号鍵KSEN0で暗号化し、一括応答データD64としてグループ暗号鍵管理部60に送信する。

【0122】グループ暗号鍵管理部60はルータ63およびルータ66から受信した一括応答データD64をグループ暗号鍵KSEN0で復号し、新規のグループ暗号鍵KSEN1を受信した端末T2~T6のIPアドレスを得ることができる。

【0123】このようにして、グループ暗号鍵KSEN1は、暗号通信グループ13に属する各端末に共有される。したがって、暗号通信グループ13に属する端末、たとえば端末T6が、新規のグループ暗号鍵KSEN1を用いて秘密鍵暗号方式で通信データを暗号化し、暗号通信グループ13に属する端末にマルチキャスト送信した場合には、端末T2~T5は、グループ暗号鍵KSEN1で受信したデータを復号することができる。

【0124】また、グループ暗号鍵管理部60が、新たなグループ暗号鍵KSEN2を生成したときには、グループ暗号鍵KSEN1で新たなグループ暗号鍵KSEN2を暗号化して配送することができ、配送応答、一括応答もグループ暗号鍵KSEN1で暗号化することができる。

【0125】この実施の形態3では、グループ暗号鍵KSEN1が配送された場合に、暗号通信グループ13に属する端末T2~T6は、グループ暗号鍵管理部60に直接配送応答をするのではなく、各端末からルータに配送応答をし、ルータが端末の配送応答データをまとめ、一括してグループ暗号鍵管理部60に配送応答をする。したがって、直接各端末からグループ暗号鍵管理部に配送応答をする場合に比べてネットワーク4に送信される通信量は減少し、ネットワークの負荷を少なくすることができる。

【0126】また、この実施の形態3では、新規のグループ暗号鍵KSEN1の配送応答および一括応答を既存のグループ暗号鍵KSEN0で暗号化している。したが

って、グループ暗号鍵の配送応答のセキュリティを高めることができ、また、グループ暗号鍵の更新を容易に行うことができる。

【0127】なお、この実施の形態3では、配送応答データD63および一括応答データD64に配送済み端末IPアドレスを有していたが、必ずしもIPアドレスである必要はなく、グループ暗号鍵管理部で端末を識別する固有の番号でもよい。たとえば、IPアドレスのかわりに、MACアドレスや、端末の製造番号を用いても同様の効果を奏することができる。

【0128】

【発明の効果】以上説明したように、この発明によれば、中継手段は、グループ暗号鍵管理手段が送信した鍵配送データに、自中継手段のアドレスを付加して各端末に配送し、各端末は、受信したデータに付加されたアドレスをもとに、自端末の情報を含む配送応答データを中継手段に送信し、中継手段は、端末から受信した配送応答データをもとに、グループ暗号鍵を受信した端末の情報をまとめ、一括応答データとしてグループ暗号鍵管理手段に送信するので、ネットワークへの負担を軽減することができるという効果を奏する。

【0129】つぎの発明によれば、中継手段はグループ暗号鍵を受信した端末の情報を暗号化してグループ暗号鍵管理手段に送信し、グループ暗号鍵管理手段は、中継手段からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができるので、グループ暗号鍵を受信した端末の情報を外部に知られることなく、安全にグループ暗号鍵管理手段に送ることができるという効果を奏する。

【0130】つぎの発明によれば、各端末は、グループ暗号鍵を受信した場合に自端末の情報を暗号化して中継手段に送信し、中継手段は、各端末からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができるので、端末の情報を外部に知られることなく、安全に中継手段に送ることができるという効果を奏する。

【0131】つぎの発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、秘密鍵暗号方式で暗号化され、送受信されるので、グループ暗号鍵を受信した端末の情報を安全かつ簡易に送信することができるという効果を奏する。

【0132】つぎの発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、公開鍵暗号方式で暗号化され、送受信されるので、グループ暗号鍵を受信した端末の情報をより安全に送信することができるという効果を奏する。

【0133】つぎの発明によれば、グループ暗号鍵が更新される場合に、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、使用していたグループ暗号鍵で暗号化され、送受信されるので、新規のグループ暗号鍵の配送と、新規のグルー

プ暗号鍵を受信した端末の情報の送信を安全に行うことができ、グループ暗号鍵の更新を安全かつ容易に行うことができるという効果を奏する。

【0134】つぎの発明によれば、中継手段は、グループ暗号鍵管理手段が送信した鍵配送データに、自中継手段のアドレスを付加して各端末に送信し、各端末は、受信したデータに付加されたアドレスをもとに、自端末の情報を含む配送応答データを中継手段に送信し、中継手段は、端末から受信した配送応答データをもとにグループ暗号鍵を受信した端末の情報をまとめ、一括応答データとしてグループ暗号鍵管理手段に送信するので、ネットワークへの負担を軽減することができるという効果を奏する。

【0135】つぎの発明によれば、中継手段はグループ暗号鍵を受信した端末の情報を暗号化してグループ暗号鍵管理手段に送信し、グループ暗号鍵管理手段は、中継手段からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができるので、グループ暗号鍵を受信した端末の情報を外部に知られることなく、安全にグループ暗号鍵管理手段に送ることができるという効果を奏する。

【0136】つぎの発明によれば、各端末は、グループ暗号鍵を受信した場合に自端末の情報を暗号化して中継手段に送信し、中継手段は、各端末からの情報を復号してグループ暗号鍵を受信した端末の情報を得ることができるので、端末の情報を外部に知られることなく、安全に中継手段に送ることができるという効果を奏する。

【0137】つぎの発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、秘密鍵暗号方式で暗号化され、送受信されるので、グループ暗号鍵を受信した端末の情報を安全かつ簡易に送信することができるという効果を奏する。

【0138】つぎの発明によれば、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、公開鍵暗号方式で暗号化され、送受信されるので、グループ暗号鍵を受信した端末の情報をより安全に送信することができるという効果を奏する。

【0139】この発明によれば、グループ暗号鍵が更新される場合に、一括応答データに含まれる端末の情報、および配送応答データに含まれる自端末の情報は、使用していたグループ暗号鍵で暗号化され、送受信されるので、新規のグループ暗号鍵の配送と、新規のグループ暗号鍵を受信した端末の情報の送信を安全に行うことができ、グループ暗号鍵の更新を安全かつ容易に行うことができるという効果を奏する。

【図面の簡単な説明】

【図1】 この発明の実施の形態1である暗号通信システムの構成を示す図である。

【図2】 図1に示した鍵配送データD1、鍵配送終端データD2、配送応答データD3、一括応答データD4

を説明する図である。

【図3】 図1に示した暗号通信システムのタイミングシーケンスを説明する図である。

【図4】 この発明の実施の形態2である暗号通信システムの構成を示す図である。

【図5】 図4に示した暗号通信システムのタイミングシーケンスを説明する図である。

【図6】 この発明の実施の形態3である暗号通信システムの構成を示す図である。

【図7】 図6に示した暗号通信システムのタイミングシーケンスを説明する図である。

【図8】 従来の暗号通信システムの構成を示す図である。

【図9】 図8に示したグループ暗号鍵管理部801の動作を説明するフローチャートである。

【図10】 図8に示した端末の動作を説明するフローチャートである。

【図11】 グループ暗号鍵リストを説明する図である。

【符号の説明】

1, 40, 60 グループ暗号鍵管理部、2, 61 鍵配送部、3, 41, 62 グループ端末管理部、4 ネットワーク、5, 8, 42, 44, 63, 66 ルータ、6, 9, 64, 67 アドレス付加部、7, 10, 43, 45, 65, 68 一括応答部、11, 12 LAN、13 暗号通信グループ、D1, D61 鍵配送データ、D2, D62 鍵配送終端データ、D3, D5, D63 配送応答データ、D4, D6, D64 一括応答データ、T1~T7 端末、t2~t6, t42~t46, t62~t66 暗号鍵管理部、KSE, KSEN0, KSEN1, KSEN2 グループ暗号鍵、KCC 暗号鍵、KS40, KS42, KS44 秘密鍵、KP40, KP42, KP44 公開鍵。

【図2】

D1 鍵配送データ				
送信元 IPアドレス	宛先 IPアドレス	データ 種別	グループ 識別子	グループ暗号鍵 データ
グループ暗号鍵 管理部1 のIPアドレス	暗号通信グループ13の IPマルチキャスト アドレス	鍵配送	ID13	KSE

【図11】

端末12: Y12	801
端末13: Y13	
端末14: Y14	
端末21: Y21	
端末22: Y22	

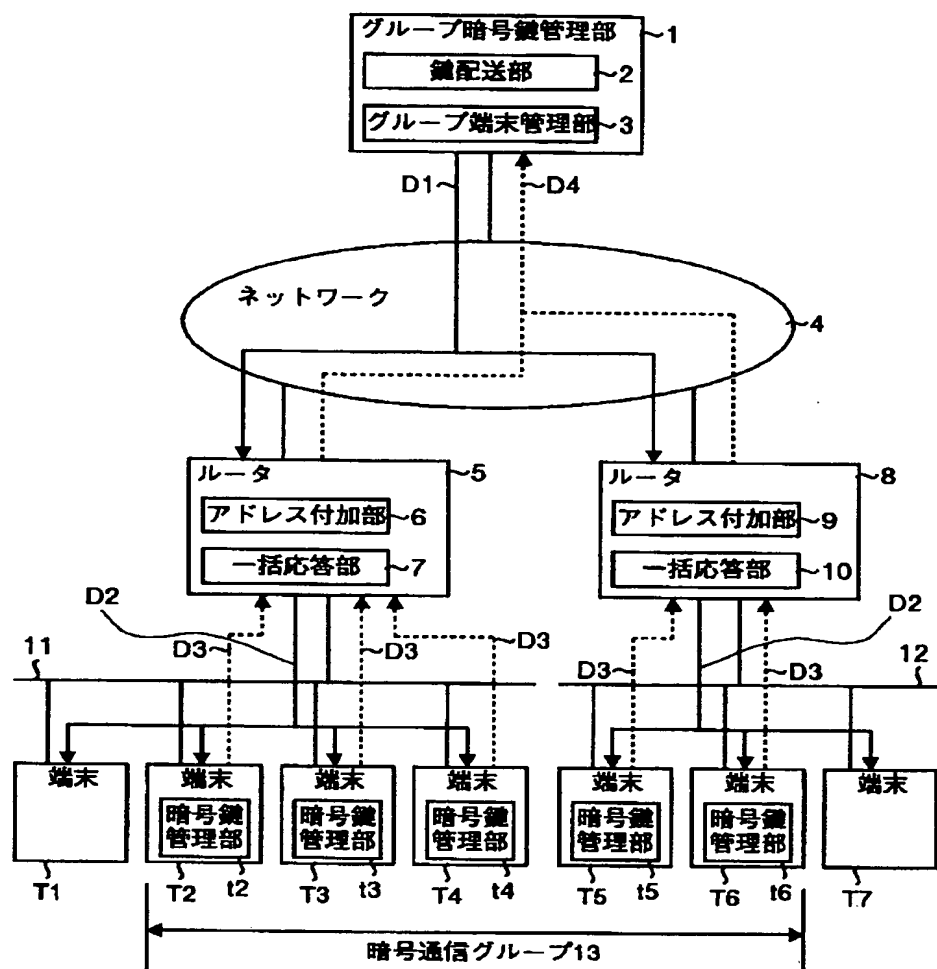
D2 鍵配送終端データ					
送信元 IPアドレス	宛先 IPアドレス	データ 種別	グループ 識別子	グループ暗号鍵 データ	代理応答 アドレス
グループ暗号鍵 管理部1 のIPアドレス	暗号通信グループ13の IPマルチキャスト アドレス	鍵配送 終端	ID13	KSE	ルータの IPアドレス

D3 配送応答データ				
送信元 IPアドレス	宛先 IPアドレス	データ 種別	グループ 識別子	配送済み端末 IPアドレス
端末のIPアドレス	ルータの IPアドレス	配送 応答	ID13	端末の IPアドレス

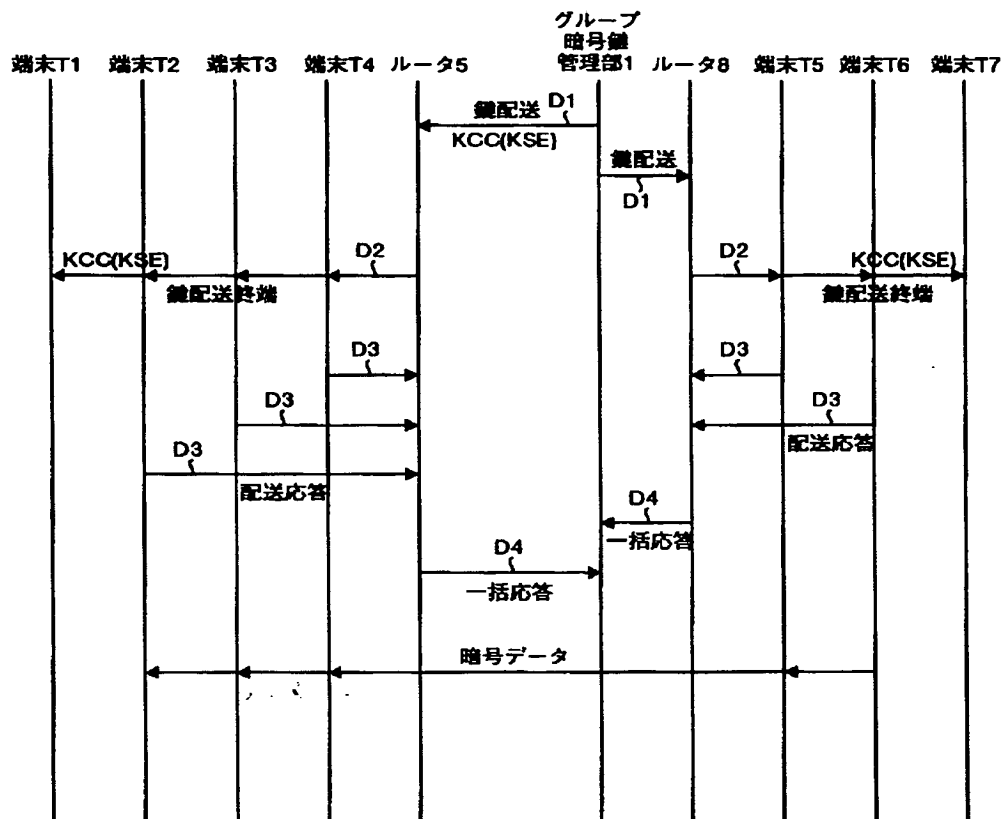
D4 一括応答データ							
送信元 IPアドレス	宛先 IPアドレス	データ 種別	グループ 識別子	配送済み 有効数	配送済み端末複数 IPアドレス		
ルータ5の IPアドレス	グループ暗号鍵 管理部1のIPアドレス	一括 応答	ID13	3	端末T2の IPアドレス	端末T3の IPアドレス	端末T4の IPアドレス



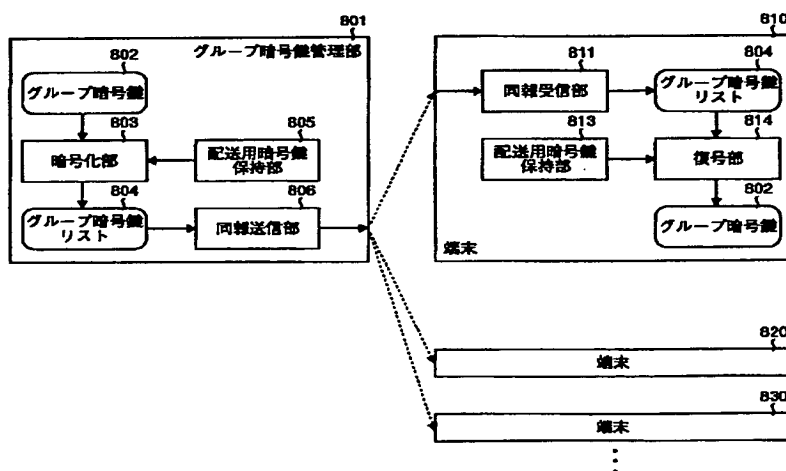
【図1】



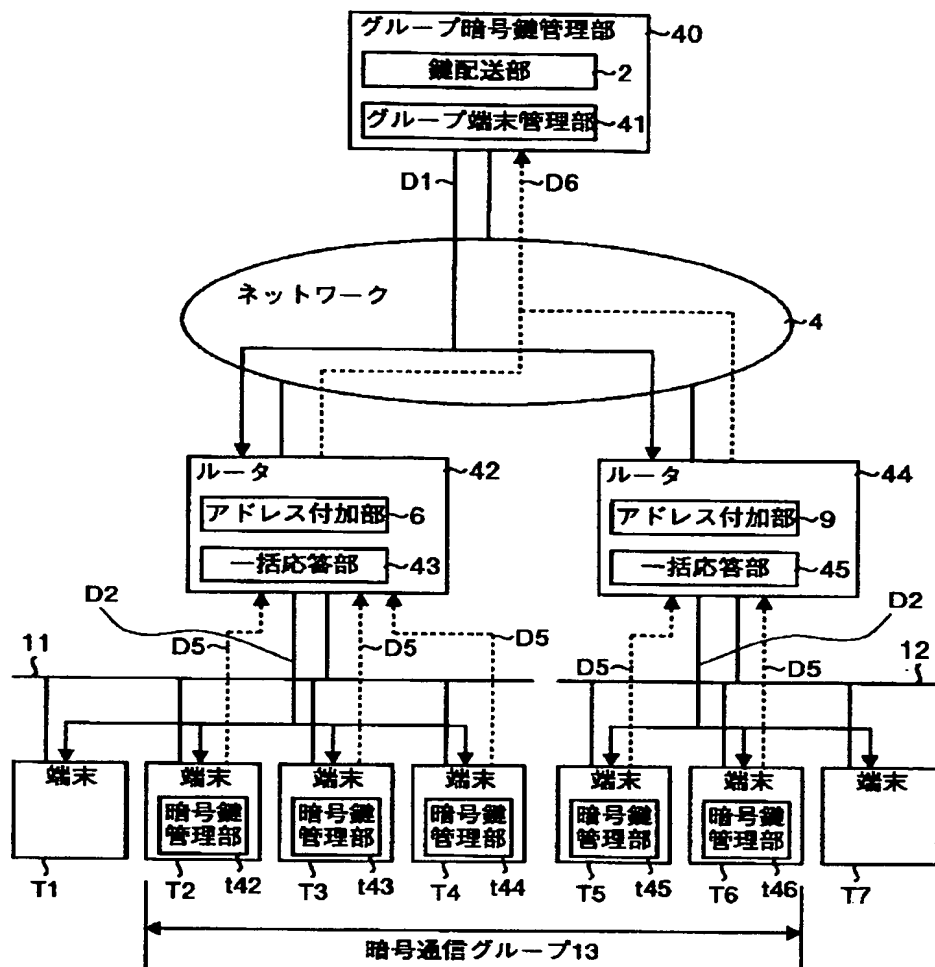
【図3】



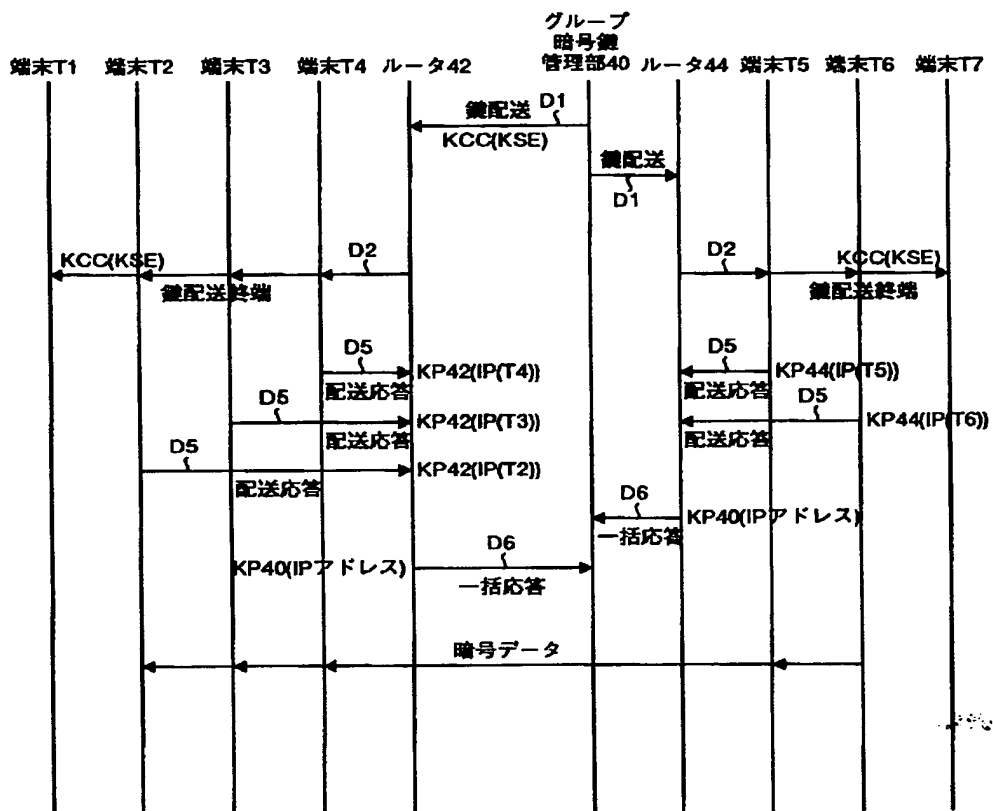
【図8】



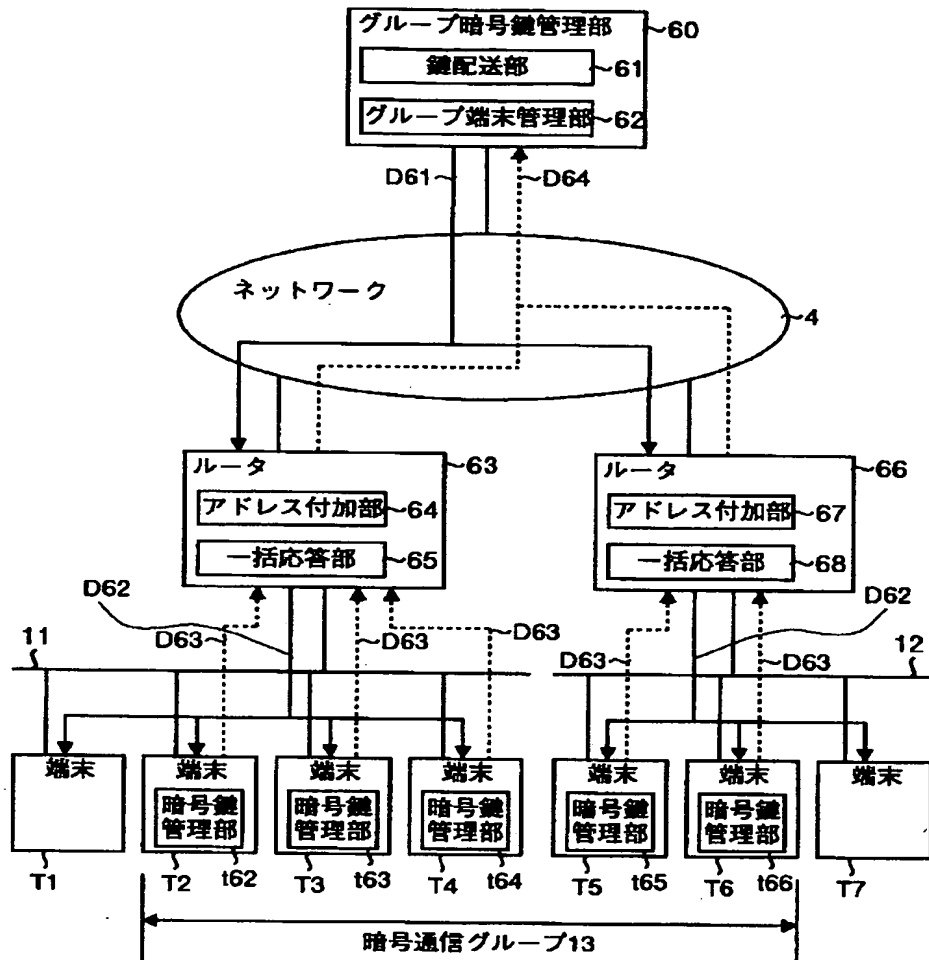
【図4】



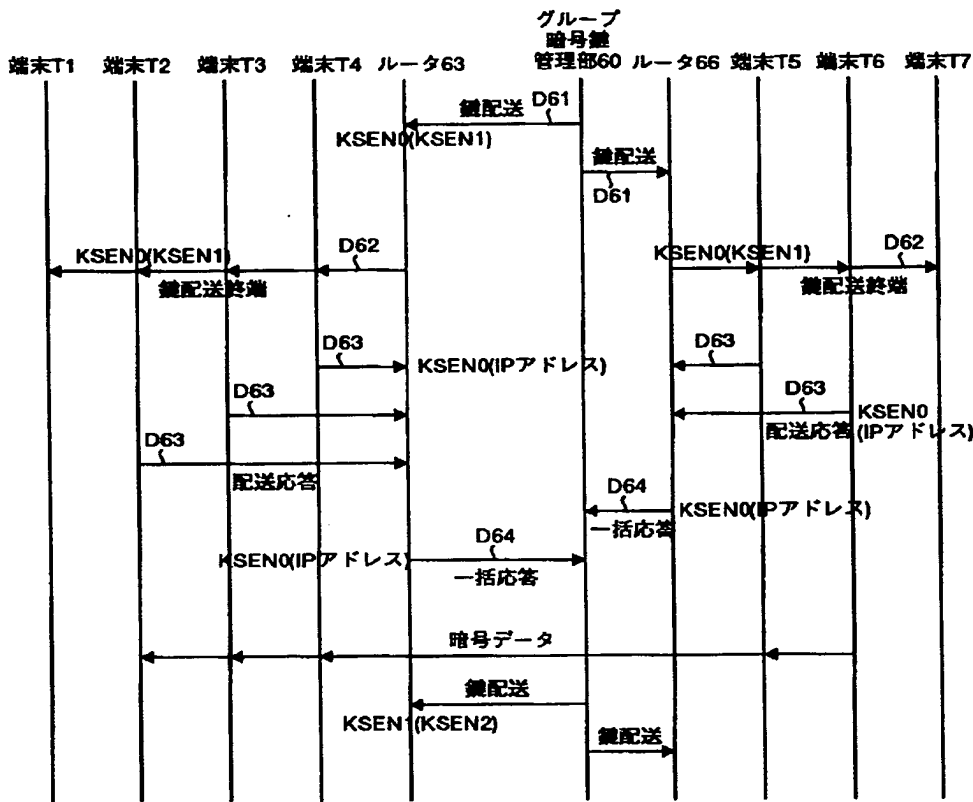
【図5】



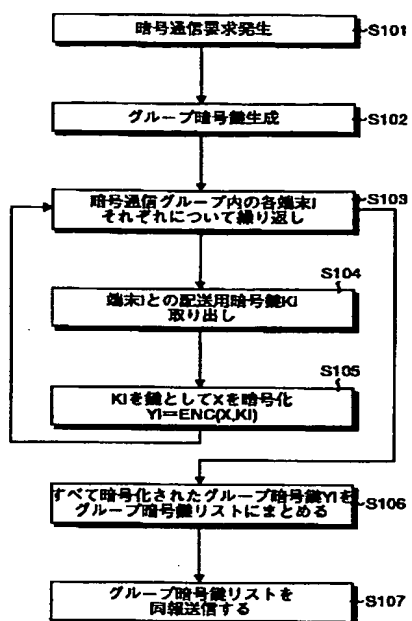
【図6】



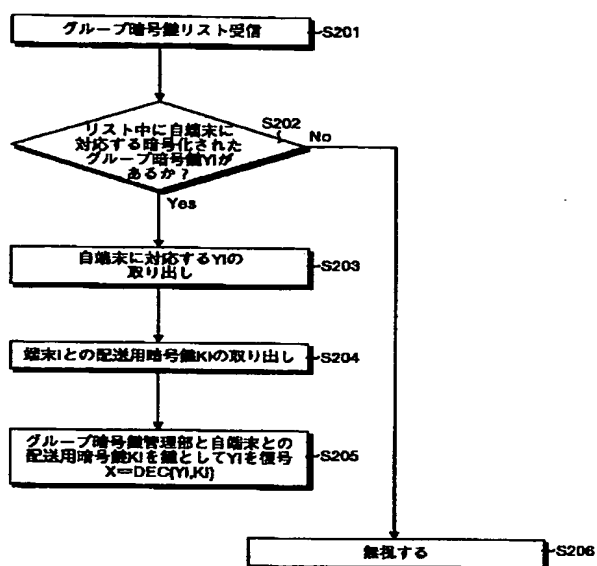
【図7】



【図9】



【図10】



**This Page Blank (uspto)**